EXHIBIT 4

FAQ

Frequently asked questions about the Taro protocol.

Taro

What is Taro?

Taro is a novel Taproot-based protocol that defines how assets can be issued/used on the bitcoin blockchain. Assets issued with the Taro protocol are held in bitcoin utxos and are transferred as part of regular bitcoin transactions.

What can I do with Taro?

Taro lets you issue all kinds of assets on bitcoin, both unique and fungible. There are no technical limits to what these assets can represent, including stablecoins, shares, tickets, ownership rights or art. Assets can be programmed using Taro's asset scripts, allowing for a broad range of functionality similar to bitcoin transactions. From an initial protocol design and prioritization perspective, Lightning Labs is focused on stablecoins' use cases first.

How does Taro work?

Taro uses Merkle trees known as a 'Merkle Sum, Sparse Merkle Tree (MS-SMT)' and Taptweak to commit to information defining an asset's creation and ownership.

What does Taro have to do with Taproot?

Taro requires Taproot to function efficiently, as Taptweak makes it possible to commit to arbitrary data without additional overhead on the blockchain. Taproot allows Taro to be scalable, economical, and privacy enhancing.

Where can I buy Taro tokens?

Taro is a protocol. The Taro protocol is released under the BSD-2-Clause license, also known as the "simplified BSD license," making it free to use and build upon. The best way to invest in Taro is to build on top of it.

Does Taro scale?

Taro minimizes its on-chain footprint by storing all necessary metadata off-chain. It further optimizes how UTXOs are used by allowing multiple assets to be controlled by the same output, and aggregate multiple transactions into a single UTXO. Taro on the Lightning Network vastly improves on the scalability of other on-chain or sharded off-chain protocols while allowing for the highest degree of self-sovereignty.

How do I find out what assets have been issued?

Once the protocol is released, information about asset issuance may be obtained either directly from an issuer, through a Taro universe or from Lightning Labs's products.

What is a universe?

A Taro universe is a repository of assets and their proofs. A universe may serve information about a single or multiple asset types (e.g. a specific stablecoin or all stablecoins). It may hold information about which assets have been issued, their quantity, and rules as well as hold proofs about recent transfers. The criteria for releasing this information is up to a universe or universe operator.

What is a pocket universe?

A pocket universe is a way to collectively store Taro assets and use the protocol without giving up ownership of assets. This pocket universe is a single party (or federation) maintaining a Taro commitment that includes assets that they can't unilaterally move themselves. A pocket universe controls the Taproot key to a UTXO, but not the keys to the (possibly multiple) Taro assets held in that UTXO. Asset holders can use the pocket universe to batch their transactions in an efficient manner.

Do I need the full blockchain to issue or transact assets with Taro?

Taro does not require you to keep or scan the entire blockchain. Similar to running a Lightning Network node, your Taro client only requires proofs about the existence of specific transactions relating to its assets, which can be obtained in 'Neutrino' mode, also known as BIP157.

Do I need bitcoin to issue assets with Taro?

To issue and transact Taro assets, bitcoin transactions need to be made, which generally require transaction fees paid in BTC. Each output also needs to carry with it a small number of satoshis to be valid.

How do I issue assets with Taro?

Once the initial implementation and protocol is released, anyone will be able to issue assets with Taro using a Taro client or a paid service. Once the asset has been issued and its genesis transaction is confirmed on

the blockchain, your asset is live and can be transferred or deployed into a Lightning Network channel.

Do all Taro assets have a limited supply?

When minting a Taro asset, you define its rules. It is possible to limit the total supply of your asset or to leave it uncapped to create additional assets later. These supply controls are enforced through cryptographic means in the Taro client.

How do I hold Taro assets in my wallet?

Your Taro wallet will need to store Taproot keys as well as Taro keys, plus the knowledge of which assets were held in which UTXOs. How such data is stored and backed up will be up to the wallet developer. If a user loses their asset proof information, it's possible for a Universe to serve the proof back to the user.

How do I send Taro assets on-chain?

To send Taro assets to somebody else, they will need to first provide you their Taro address. This address contains information about the asset and public keys necessary for holding the asset. The address format is designed to help prevent Taro assets from being lost or unrecoverable.

What fees do I have to pay?

Typically, a Taro transaction will carry on-chain fees, which are paid to bitcoin miners similar to a regular bitcoin transaction. When transacting Taro assets off-chain, you may pay routing fees to Lightning Network nodes instead. When using a pocket universe, grouped transactions can share on-chain fees.

Taro on the Lightning Network

How do I send Taro assets over the Lightning Network?

Taro assets can be deployed into a Lightning Network channel in a similar manner as bitcoin. When a route denominated in the relevant asset exists, the asset can be routed through it, otherwise it can be trustlessly swapped for BTC and its value is routed to the destination, where it may be swapped back or into a different asset. Ultimately, the majority of this process will be obfuscated to the end user and handled by nodes and wallets.

What is edge liquidity?

Edge liquidity describes the concept that some Lightning Network nodes, with which you have Taro asset channels, may be willing to swap their value to BTC and back, allowing you to use your Taro assets to pay for any Lightning Network invoice, or receive any asset by issuing a standard Lightning invoice.

How does Taro know how much an asset is worth?

The Taro protocol does not prescribe how edge nodes and Taro asset holders agree on a price -- though a few options can be supported. As long as both agree on a rate, any Taro asset can be swapped for BTC and its value transmitted through the broader Lightning Network.

How does Taro deal with the “optionality” challenges?

Edge nodes’ liquidity has some optionality properties, but this optionality will be priced by the market. Nodes, which offer this optionality, can decline to facilitate the quoted swap and users can avoid nodes which don’t perform frequently. Ergo, Taro doesn’t have a “free option problem” which can exist in cross-chain atomic swaps.

Do you need an equivalent amount of bitcoin to move taro assets between channels?

The owner of a Taro asset does not need to own an equivalent amount of bitcoin to be able to send or receive amounts denominated in their asset. However, a route must exist between the sender and receiver with sufficient liquidity -- either in bitcoin or the Taro asset.

Custody and redeemability in the Taro protocol

		User holds the keys to the taproot UTXO	
		🔑 Yes	🚫 No
User holds Taro asset keys	🔑 Yes	Full self-custody	User is **using** a pocke universe
	🚫 No	User is **operating** a pocket universe	Entirely custodial relationship

← Previous
Taro on Lightning

Next - Lightning Network Tools
LND →

Last modified 5mo ago

WAS THIS PAGE HELPFUL?